Brian Ta | CSCE 313

Homework 3

1) DNS maps hostnames to IP addresses and vice versa, which is needed for an application to connect to it. The program will use the IP address to complete the request to connect. Multiple returning of IP address results from a hostname having multiple IP addresses for its record.
2) The shutdown command acts on the file descriptor of the socket to shut down its connection. It differs from close by having a second argument which specifies the type of shutdown which disables subsequent send and/or receive operations depending on the value of the argument. Using close destroys the socket completely. One can use shutdown in the following scenario: if you are finished sending data but want to continue receiving data (and vice versa), using shutdown with the correct second argument can handle this whereas close does not.
3) TCP offers full reliability in protocols which UDP does not offer.
4) Yes, you can configure a browser in such way. The advantages of having many TCP connections is that it guarantees reliable data transmission in all of those connections. A main disadvantage is performance under mass data congestion - since TCP offers data congestion control, a congestion with all of the connections may delay data transfer.
5)
    a) A(1111) → S(8888)
    b) B(2113) → S(8888)
    c) S(8888) → A(1111)
    d) S(8888) → B(2113)
    e) Yes since they are unrelated.
    f) No since different port numbers indicate different hosts.
6)
    a) TCP Slow Start on intervals 1-6, 23-27
    b) TCP Congestion Avoidance: 6-16, 17-22
    c) Triple duplicate ACK after the 16th transmission round
    d) Ssthreshold at 1st: 32
    e) Ssthreshold at 18th: 21
    f) Ssthreshold at 24th: 13
    g) 70th segment sent during round 7
    h) 8/2 = 4

7) Confidentiality is the idea that a message cannot be determined by an attacker who obtains an encrypted message. Message integrity is the idea that the receiver of the message knows if the message was changed during transmission. Yes, you can have one without the other - the case where a receiver is given a confidential message where the message had been changed without detection (Non-integrity) and vice versa.

8) N(N-1)/2 Pairs ⇒ N(N-1)/2 Keys. With public key encryption, 2N keys are needed.

9) RSA with p = 3 and q = 11
   - N = 3*11 = 33, (p-1)(q-1) = 20
   - Choose k_e = 7 then k_d = 3 since $k_e k_d$ mod 20 = 1
   - ⇒ Public Key (7, 33); Private Key (3, 33)
   - h e l l o → 8 5 12 12 15
   - Encrypting “hello” with public key:
     - h: 8^7 mod 33 = 2
     - e: 5^7 mod 33 = 14
     - l: 12^7 mod 33 = 12
     - l: 12^7 mod 33 = 12
     - o: 15^7 mod 33 = 27
   - Decryption of the ciphertext with private key
     - 2: 2^3 mod 33 = 8 → h
     - 14: 14^3 mod 33 = 5 → e
     - 12: 12^3 mod 33 = 12 → l
     - 12: 12^3 mod 33 = 12 → l
     - 27: 27^3 mod 33 = 15 → o